What is claimed is:

1. In a network carrying a plurality of packets over at least one network link, said network including a computer, a first network component having memory and a processor and configured to store information in said memory about at least one of said plurality of packets, and a second network component, a method for detecting a target packet comprising:

receiving said at least one of said plurality of packets over said link to obtain a received packet;

determining a hash value of at least a portion of said packet;

using said hash value to identify a location in said memory;

setting a flag in said memory, said flag associated with said location;

receiving a query message identifying a target packet at said first network component;

said first network component using said flag in processing said query message to determine if said target packet has been encountered;

creating a reply if said target packet has been encountered; and

said first network component making said reply available to said network if said target packet has been encountered;

2. The method of claim 1 and wherein making said reply available to said network includes forwarding said reply to said second network component.

3. The method of claim 2 and wherein said second network component is a computer.

4. The method of claim 1 and wherein said reply contains a network address for said first network component.

5. The method of claim 1 and wherein said hash value is determined over the entire packet.

6. The method of claim 1, further comprising:

determining if said received packet has undergone a transformation, such transformation having occurred if a first hash value of at least a portion of said packet computed at a first time is not equal to a second hash value of at least a portion of said packet computed at a second time, said second time occurring after said first time.

7. The method of claim 1 and wherein said network is an Internet Protocol (IP) network.

8. The method of claim 1 and wherein said link is a wireless link.

9. The method of claim 1 and wherein said first network component is a router.

10. In a network carrying a plurality of packets over at least one link, said network including a network component operatively coupled to said link and having a memory and a processor, a method for storing information about a plurality of packets received over said network, at least a portion of said information being used to locate an intrusion point for a first one of said plurality of packets, said method comprising:

receiving said first one of said plurality of packets;

determining a first hash value of said first one of said plurality of packets over at least a portion thereof;

using said first hash value to identify a first location in said memory;

setting a flag at said first location said flag indicating said first hash value has occurred;

receiving a second one of said plurality of packets;

processing said second one of said plurality of packets to obtain information contained therein;

using said information contained in said second one of said plurality of packets to determine if said first one of said plurality of packets has been observed; and

making a reply available to said network if said information contained in said second one of said plurality of packets indicates that said first one of said plurality of packets has been observed, said reply capable of being used as part of a method for locating said intrusion point for said first one of said plurality of packets.

11. In a network carrying a plurality of packets over at least one link, said network including a network component operatively coupled to said link, a method of using a configurable packet to inhibit an intrusion of a target packet into said network, said method comprising:

receiving said configurable packet at said network component, said configurable packet comprising:

a body portion comprising information about said target packet and machine-readable instructions for causing said network component to modify its operation after executing said instructions;

processing said configurable packet to extract said information and said instructions; and

executing said instructions to cause said network component to modify its operation in a manner such that said intrusion into said network is inhibited.

12. The method of claim 11 and wherein said information is a hash value.

13. In a network carrying a plurality of packets over at least one link, said network including a plurality of devices and a system operatively coupled to said link, said system for assisting with the location of an intrusion point of a target packet in said network, said system comprising:

a first interface for receiving at least one of said plurality of packets to obtain at least one received packet;

a second interface for placing a subset of said at least one received packet onto said link;

a bus communicatively coupled to said first interface and said second interface;

a memory communicatively coupled to said bus, said memory storing information about said at least one received packet in a machine-readable form;

a processor communicatively coupled to said bus and said memory, said processor executing machine-readable instructions for processing said at least one received packet;

a plurality of first hash values, each one of said plurality of first hash values determined from said at least one received packet respectively;

a second hash value determined from at least a portion of said target packet; and

a reply made available to certain of said devices in said network using said second interface, said reply made in response to comparing said second hash value to each one of said plurality of first hash values.

14. The system of claim 13 and wherein said first interface and said second interface are combined into a single bi-directional interface.

15. The system of claim 13 and wherein said reply is made available to another network.

16. The system of claim 13 and wherein said network is a wireless network.

17. The system of claim 13 and wherein said network is an Internet Protocol (IP) network.

18. The system of claim 13 and wherein said processor is an ASIC.

19. The system of claim 13 and wherein said reply is a positive reply if said second hash value matches at least one of said plurality of first hash values.

20. The system of claim 13 and wherein said reply is forwarded to those of said devices one hop away.

21. In a network component operatively coupled to a network by at least one link carrying a plurality of packets, a computer-readable storage medium containing executable code for instructing a processor to process information about at least one of said plurality of packets, said information used to facilitate locating an intrusion location for a malicious packet in said network, said executable code instructing said processor to perform operations comprising:

determining a hash value for at least a portion of said at least one of said plurality of packets;

using said hash value to form an index into a memory containing a plurality of memory locations, said memory further used for storing first information about a subset of said plurality of packets;

setting a flag at one of said memory locations, said flag corresponding to said index;

receiving a query containing second information about said malicious packet and extracting said second information therefrom;

comparing said second information about said malicious packet to the contents of said memory; and

generating a reply if said second information matches said contents stored at one of said plurality of memory locations, said reply indicating that said intruding packet has been observed by said network component.

22. In a device operatively coupled to a network, a computer-readable data signal for modifying the operation of said device to prevent propagating an intruding packet through said network after receiving and processing said signal, said signal comprising:

a header portion; and

a body portion comprising:

information derived from at least a portion of said intruding packet; and

machine-readable instructions executed by said device to prevent propagating said intruding packet through said network.

23. In a device operatively coupled to a network, a computer-readable data signal having a body portion for use in identifying an ingress location of a target packet in said network, said body portion comprising:

a hash value identifying said target packet as detected by said device, said hash value of said target packet having been computed by said device; and

identification information about said device.

24. The computer-readable data signal of claim 23 further comprising a header portion, said header portion comprising:

a network address.

25. In a network including a source component, a server and a destination component, a plurality of routers each having a memory, said routers used in detection of a malicious packet intruding into said network through said source component, comprising:

each of said routers including an input means for receiving at least a number of said packets;

said each of said routers further including means for processing and storing selected first information about each of said at least a number of said packets;

said each of said routers further including means for outputting at least a subset of said each of said at least a number of said packets;

said processing and storing means further including means for determining a hash value for each of said at least a number of said packets respectively and for storing a representation of said hash value into said memory;

said input means further including means for receiving query messages from said server and for extracting second information about said malicious packet;

said each of said routers further including means for comparing said representation with said second information to determine a match therebetween;

said each of said routers further including means responsive to operation of said comparing means determining said match for generating a first reply packet to be

forwarded to both said server and to those of said plurality of routers displaced one hop away from said each of said routers; and

said each of said routers further including means responsive to operation of said comparing means determining no match for generating a second packet to be forwarded to said server indicating said malicious packet was not observed.